DOCKET FILE COPY ORIGINAL

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

IN THE MATTER OF:	)	
	)	
Communications Assistance	)	**CC Docket No. 97-213**
For Law Enforcement Act	)	
(CALEA)	)	

COMMENTS OF SBC COMMUNICATIONS INC.

JAMES D. ELLIS
ROBERT M. LYNCH
DURWARD D. DUPRE
LUCILLE M. MATES
FRANK C. MAGILL

ATTORNEYS FOR
SBC COMMUNICATIONS INC.
175 E. HOUSTON
Room 1258
San Antonio, Texas 78205
(210) 351-3428

December 12, 1997

Summary

SBC strongly supports efficient implementation of CALEA consistent with the goals of Congress and with reimbursement of the costs by the Government, and, if necessary, by ratepayers. However, the FCC must not require carriers to provide expanded surveillance capabilities where Congress has not so directed. Congress, not the FCC, should clarify whether and to what extent expanded surveillance capabilities requested by law enforcement agencies ("LEA") are included in CALEA. The FCC must also recognize that carriers cannot reasonably be expected to modify their equipment, facilities and services, if necessary for CALEA compliance, until standards are adopted and equipment to implement those standards becomes commercially available.

All telecommunications carriers should be equally subject to CALEA's requirements. This includes resellers, carriers purchasing unbundled network elements from facility carriers, and small carriers. Nothing in CALEA suggests that the burdens imposed on carriers are intended to be differentiated according to the carrier's size. However, the FCC should minimize the administrative burden on the entire industry by extending to all carriers the NPRM's proposal that small carriers only file a Statement of Compliance. Common carriers that provide information services should be subject to CALEA only to the extent of their capacity as common carriers.

The FCC should not impose rules regulating carriers' internal authorization procedures. Rules for "appropriate authorization" for CALEA are already set out in Title 18 of the US Code and these effectively protect against unlawful surveillance. If the FCC nonetheless adopts specific requirements for internal authorization, carriers with effective internal authorization controls should be deemed in compliance. There is no basis to hold carriers vicariously liable when employees exceed their scope of employment and willfully disregard carriers' policies prohibiting unauthorized interception or disclosure.

Requiring carriers to report compromises of confidentiality and of illegal wiretapping to the FCC is an unnecessary administrative burden given the historically rare incidence of such breaches. Compliance with reporting will not mitigate carriers' liability under 18 U.S.C. §2511 or §2520. Such reporting, in fact, may violate a court or other legal authority's nondisclosure order.

The FCC should not construe the requirements for "appropriate authorization" to prohibit carriers from undertaking preparatory activity prior to the actual receipt of a court order or other legal authority for surveillance. First, not all surveillance activity must meet the detailed requirements described by the FCC. Imposing all of the requirements of a Title III order on every surveillance would cause a severe and unwarranted burden on LEAs and carriers. Moreover, such requirements would cause delays in implementing lawful surveillance, to the detriment of LEAs' investigations.

Record keeping requirements should be limited to only that information necessary to further Congressional goals. Moreover, the FCC should neither limit the number of employees that participate in lawful surveillance, nor require lists to be kept of those employees. The sheer number of employees who may need to be involved in effectuating lawful surveillance makes these requirements unrealistic. Similarly pre-surveillance affidavits would be overly burdensome and unnecessary as would the requirement for records to be generated contemporaneously with or within 48 hours of the initiation of surveillance. Carriers should be permitted to continue using their previously established and successful record-keeping formats and methods for preserving confidentiality and protecting against unlawful interception activity which were developed to comply with existing legal requirements. Similarly, carriers should continue to provide LEAs with employee contact information but that information should be limited to the employee's name, title and contact number.

The FCC properly defers its involvement with the development of technical standards. The FCC should permit the industry, existing standards setting bodies and LEAs to continue their efforts. However, continued delay in reaching standards may require Commission intervention to facilitate or accelerate the parties' decision making. Moreover, delay will likely require the Commission to grant extensions or waivers of compliance dates. Those should be blanket waivers or company wide extensions. The FCC should also confirm SBC's interpretation that the FCC's network disclosure requirements do not apply to carriers' CALEA related network changes. If any change triggers a network disclosure obligation, the FCC should grant carriers a limited exemption given LEAs' needs to avoid public disclosure of the availability of CALEA changes.

The FCC's interpretation of "reasonably achievable" will determine the Government's fiscal responsibility for assistance capability. Therefore, the FCC's criteria should ensure Congress' intent that costs be equitably distributed. The evaluation of "reasonably achievable" should be applied to equipment facilities or services on a carrier-by-carrier basis, by each type of platform. The FCC should give minimal weight to the financial resources of the carrier and the extent to which the design and development of the equipment facilities or service was initiated before January 1, 1995. Primary weight should be given to the reasonable availability of technology and the implementation cost per affected switch. The FCC should also clarify that "deployed" means that a particular switch platform is commercially available, regardless of whether a carrier has actually installed it in the network. Costs of modifications that are not found to be reimbursable by the Government should be recovered through the normal rate making process.

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

IN THE MATTER OF:	)	
	)	
Communications Assistance	)	**CC Docket No. 97-213**
For Law Enforcement Act	)	
(CALEA)	)	

COMMENTS OF SBC COMMUNICATIONS INC.

I. Introduction.

SBC Communications Inc., ("SBC"), on behalf of its subsidiaries, hereby submits the following Comments in response to the FCC's Notice of Proposed Rulemaking ("NPRM") in the above-numbered Docket, issued on October 10, 1997.

Since the enactment of the Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. §1001, *et seq.*, SBC has been actively involved in all phases of the implementation process, including participation in the development of industry standards for both wireline and wireless services and in the series of discussions between the industry and the Federal Bureau of Investigation ("FBI"). While this process is far from completed, and notwithstanding certain continuing disagreements between the FBI and the telecommunications industry concerning the appropriate interpretation and application of some provisions of CALEA, SBC strongly supports efficient implementation of CALEA consistent with the goals of Congress and with reimbursement of the costs of such implementation from the government and, if necessary, rate payers.

SBC and its subsidiaries have a long and active history of cooperating with and assisting law enforcement in conducting court-approved electronic surveillance, and currently no problems exist in carrying out this service in a timely, accurate and efficient manner. SBC believes this is generally true throughout the industry, and that, accordingly, there is no need for the FCC to establish a new layer of administrative rules or regulations that merely add costs to the process without furthering the intent of Congress in enacting CALEA.

It is critical that the FCC, in developing its regulations under CALEA, be mindful of the primary objectives of Congress as expressed in CALEA and its legislative history, and as acknowledged in Paragraph 5 of the NPRM, *i.e.*, to preserve a narrowly focused capability for the FBI and state and local law enforcement agencies ("LEAs") to conduct properly authorized electronic surveillance, while protecting the privacy of communications not authorized to be intercepted, and avoiding impedance of the development of new communication services and technology. Many, if not most, of the continuing disagreements between the industry and the law enforcement community over CALEA implementation arise directly from the fact that the FBI and other LEAs persist in attempting to use CALEA to expand the scope of their surveillance capabilities. This is not what Congress intended, nor is it consistent with the assurances given to Congress by FBI Director Freeh in his Congressional testimony prior to CALEA's enactment, to the effect that CALEA's framers did not seek to expand

surveillance capabilities, but rather sought only to preserve the *status quo ante* in the face of changing technology.[1]

As pointed out in Paragraph 8 of the NPRM, the language of CALEA specifically prohibits LEAs or officers from requiring and/or prohibiting adoption of any specific design of equipment, facilities, services, features, or system configurations. 18 U.S.C. §1002(b)(1). Nevertheless, LEAs, led by the FBI, continue to insist that, in order to be in compliance with CALEA, the pending industry standards for CALEA implementation must provide for carriers to configure their networks to furnish LEAs with a number of advanced surveillance capabilities that have never before been available. These advanced capabilities comprise what has become generally known as the FBI's "punch list". Because these are new capabilities which may have become feasible only due to recent technological advances, and because CALEA contains no mandate to expand the scope of electronic surveillance, SBC is concerned that, in light of the non-expansionist intent of CALEA, providing LEAs with "punch list" capabilities could expose SBC to potential civil liability under the Federal wiretapping and/or civil rights statutes[2].

---

[1] Testimony of Louis J. Freeh, Director, FBI, March 18, 1994, before the Senate Judiciary Committee, Subcommittee on Technology and the Law, and the House Judiciary Committee, Subcommittee on Civil and Constitutional Rights.

[2] Respectively, 18 U.S.C. §2520 and 42 U.S.C. §1983. One example from the "punch list" illustrates clearly the source of this concern. If a surveillance target, *i.e.* a person whose telephone communications are being intercepted pursuant to a proper court order, participates in a three-way conference call with two people who are not themselves the subjects of any court-ordered interception, and the target party "drops off" the three-way call, the FBI insists that carriers provide it with the ability to continue monitoring any further conversation between the non-target parties. Given these facts, SBC is concerned that the non-target parties could have a claim under 18 U.S.C. §2520 against both the FBI and the carrier for unlawfully intercepting their communications. To varying degrees, each of the "punch list" items presents similar liability concerns for SBC and other carriers.

In addition, the cost of including the "punch list" items in the pending standards could prove to be prohibitive. Recent industry testimony before a U.S. House of Representatives subcommittee showed that, for a switch-based CALEA solution, the cost of software development alone likely would be doubled, possibly reaching more than $2 billion industry-wide, by inclusion of the "punch list."[3]

Accordingly, SBC believes that, before any of the "punch list" capabilities can reasonably be included in any industry standard, and before any such capabilities can be developed and implemented in any carrier's network, Congress must clarify whether and to what extent these capabilities were even envisioned, as well as whether they are to be included in CALEA's mandate to the industry.

In addition to the foregoing concerns, the FCC should take into consideration the fact that carriers cannot reasonably be expected to move forward with modifications to their equipment, facilities and services, if any are needed to become CALEA-compliant, until standards are adopted and equipment to implement those standards becomes commercially available. Given the delay in establishing standards, the current deadlines established by Congress may prove impossible to meet. The industry estimates it could take at least 30 months after the standards have been finalized to implement CALEA-related switch upgrades, including 24 months for software development and 6 months for testing, installation and deployment. Progress with CALEA

[3] Testimony of Roy Neel, President & CEO of USTA, October 23, 1997 before the House Judiciary

implementation is further impeded by the need to resolve issues of the equitable distribution and reimbursement of costs that must be incurred to implement those standards.

II. All Telecommunications Carriers Should Be Equally Subject To CALEA's Requirements, Including Small Carriers. However, The FCC Should Minimize The Administrative Burden On The Industry By Extending To All Carriers The NPRM's Proposal For Small Carriers.

A. Carriers Subject To CALEA's Requirements.

Section 102(8) of CALEA (47 U.S.C. §1001(8)) defines "telecommunications carrier" as including a "person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire." SBC supports the FCC's tentative conclusion that all entities are subject to CALEA requirements to the extent that they offer telecommunications services to the public. (NPRM, Paragraph 17.) This includes common carriers, CLECs, CAPs, CMRS providers, cable operators and electric and other utilities to the extent that they offer telecommunications services. The Commission should also interpret "telecommunications carrier" to include entities that may not be facility-based carriers. Resellers, for example, should be subject to all CALEA obligations because each reseller will be the carrier of record with respect to its customers, and thus will be in sole possession of information to which the network carrier normally will not have access, such as customer identifying information and billing information. Further, some resellers provide elements of their own network infrastructure and

---

Committee, Subcommittee on Crime.

should be subject to the CALEA capacity and capability requirements, depending upon the nature of the infrastructure involved. Although the reseller's service may be provided over a network carrier's facilities, and the network carrier will actually facilitate the court-ordered surveillance, the reseller again will have exclusive access to billing and other data that may be necessary for compliance with the court order. Therefore the reseller should be an initial recipient of any court orders affecting its customers, in addition to the network carrier from which the reseller obtains its lines. (NPRM, Paragraph 17.)

For the same reason, carriers that purchase unbundled network elements (UNEs) should also be subject to CALEA. Like resellers, these carriers will also be the carrier of record for their customers and will have billing and other data that may be part of the customer and call-identifying information required by the LEA seeking to conduct court-ordered surveillance. On the other hand, carriers that provide their own switches and purchase non-switch UNEs from a LEC, such as loop links, clearly fit the definition of a telecommunications carrier and should be subject to CALEA. These carriers normally will not require LEC involvement to set up CALEA-related surveillance.

Further, small carriers should be subject to CALEA's capability and administrative requirements. (NPRM, Paragraph 34.) The Congressional objectives embodied in CALEA are the same regardless of the size of the carrier, and the law's requirements must be applied equally to all carriers if such goals are to be achieved. Had Congress intended for different rules to be applied based on carrier size, it would have made its intent clear in the statute.

Similarly, the FCC's security and integrity concerns are exactly the same with respect to small carriers as with respect to large carriers. The only real distinction is that, generally, small carriers will perform fewer CALEA wiretaps. Accordingly, there should be no differing standards set for certain classes or categories of carriers. The FCC's proposal that small carriers file a statement of compliance instead of filing their policies and procedures with the FCC is an effective means to reduce the administrative burdens of the rules adopted in this proceeding, and should be applied to all carriers in order to minimize carriers' compliance costs. (NPRM, Paragraph 35.) As the FCC recognized, large carriers are likely to have acceptable policies, processes, and procedures in place. (NPRM, Paragraph 74.) In any event, regardless of a carrier's size, the FCC should only require records to be kept of information that has a clearly definable relationship to accomplishing the goals of CALEA.

B. Carriers Not Subject To CALEA's Requirements.

The Commission should be aware, however, that the listing in Paragraph 17 would not include PBX providers and aggregators, and that carriers which transport calls of PBXs or aggregators will be limited in the degree of assistance they can provide to law enforcement with respect to such calls. SBC also believes the FCC is correct in exempting entities from CALEA assistance capability obligations that exclusively provide information services. (NPRM, Paragraph 20). Information services provided by common carriers should be similarly excluded; in other words, carriers that provide information services

should be subject to CALEA only to the extent of their capacity as common carriers. This is consistent with §102 of CALEA, (47 U.S.C. §1001), which states that the term "telecommunications carrier" does not include "persons or entities insofar as they are engaged in providing information services."

SBC also agrees with the FCC's tentative conclusion that pay telephone providers are not telecommunications carriers for purposes of CALEA, because they do not offer transport or switching services to the public. (NPRM, Paragraph 16.) Pay telephone providers furnish only customer premises equipment (even if the CPE can perform advanced functions akin to certain network-type services, *i.e.*, store and forward functions). Of course, excluding pay telephone providers from CALEA responsibility does not affect their obligation to respond to court orders for selective electronic surveillance (or minimization) of pay telephone calls.

III. Existing Legal Requirements Already Effectively Protect The Privacy Of The Public's Wire, Oral And Electronic Communications, And The Security And Confidentiality Of Lawfully Authorized Surveillance.

A. "Appropriate Authorization" Does Not Refer To A Carrier's Internal Procedures; Therefore, Burdensome Rules Are Unnecessary.

SBC disagrees with the FCC's tentative conclusion that the term "appropriate authorization" as used in §229 of the Communications Act applies to internal authority granted by a carrier to its employees to effectuate lawful surveillance at the request of LEAs. There is no basis in the legislative history for such a conclusion. "Appropriate authorization" means, for purposes of both §229 and CALEA, a court order or other authorization as provided in the

applicable sections of Title 18 of the United States Code. Consequently, there is no need for the FCC to impose burdensome rules regulating carriers' internal authority procedures. If, however, the FCC interprets the "appropriate authorization" requirement of §229(b)(1) to mean that the carrier must "authorize" its employees to engage in interception activities, then companies with effective controls already in place should be deemed to be in compliance based on a "statement of compliance" filed by the carrier. The FCC should deem compliant all carriers that have: (a) dedicated employees or organizations to assist LEAs; (b) developed security and confidentiality policies; (c) provided training as to when and how authorized employees may undertake interception activities, and (d) prohibited unauthorized surveillance by their employees. Given that SBC companies process thousands of surveillance requests annually,[4] a requirement for separate authorization for each such request would be overly burdensome, and would serve no discernible purpose. (NPRM, Paragraph 25.)

B. Carriers That Establish And Enforce Internal Policies Meeting The Goals Of CALEA §105 Should Not Be Subject To Vicarious Liability When Employees Act Outside Their Scope of Employment.

SBC agrees with the tentative conclusion that CALEA §105 (47 U.S.C. §1004) requires carriers to ensure that only surveillance in accordance with a court order or other lawful authorization is performed within the carrier's switching premises. Section 105 of CALEA does not, however, require that

[4] See Note 7, infra, and accompanying text.

carrier employees with knowledge of such surveillance will not reveal the existence or content of intercepted communications to anyone other than authorized law enforcement personnel, except as required by a court of competent jurisdiction or appropriate legislative or regulatory body, as the FCC tentatively concludes. (NPRM, Paragraphs 25, 26.)[5] SBC also urges the FCC to note that CALEA §105 does not shift to carriers the Government's initial burden of ensuring that only lawful surveillance is sought and authorized in the first place, nor does it impose any duty on carriers where the interception of wire communications or access to call-identifying information is effected anywhere other than within the carrier's switching premises.

SBC believes that the nature and extent of any carrier's civil and/or criminal liability under the relevant provisions of "Title III", (18 U.S.C. §§2511 and 2520), is not affected by CALEA §105. CALEA itself contains no provision for private civil remedy if a carrier is found to be noncompliant, nor is there any hint in either the language or legislative history of CALEA of any Congressional intent that it be enforced by private civil remedies or by criminal sanctions.[6] Furthermore, it should be noted that the theory of vicarious liability assigns responsibility to employers for acts of their employees only when employees act within the scope of their employment. This well-established rule of law cannot be overridden without an explicit statement of Congressional intent, and CALEA

[5] Existing legal restrictions against disclosure of existence and contents of wiretaps, etc. are contained in 18 U.S.C. §2511.

[6] 18 U.S.C. §2522 contains the enforcement procedures for CALEA. This section provides for issuance of enforcement orders by U.S. District Courts, and for civil penalties, in actions brought by the Attorney General. The actions and penalties provided in §2522 are exclusively civil remedies.

contains no such statement. In any event, as the FCC recognizes, 18 U.S.C. §2520 provides that good faith reliance upon a court order or government attorney's certification is a complete defense against any action alleging unlawful interception of communications. It is therefore difficult to envision how CALEA §105, or any FCC rule promulgated pursuant thereto, would operate to override these statutory defenses and impose vicarious liability on a carrier unless the unlawful interception occurs within the offending employee's course and scope of employment; in other words, only if the unlawful act is authorized by the employer may the employer be held liable. Moreover, as the FCC recognizes in Paragraph 29 of the NPRM, "[t]he legislative history of CALEA contains no congressional finding that existing law is inadequate to protect citizens' privacy and security rights against improper surveillance." Accordingly, carriers that establish and strictly enforce policies prohibiting unauthorized interception and disclosure should not be subject to vicarious liability if employees exceed their authority by willfully disregarding such policies. (NPRM, Paragraph 27.)

C. Carriers Should Be Required To Report Unlawful Interceptions And Breaches Of Confidentiality Only To The Affected Court or LEA.

With respect to the merits of the proposal in Paragraph 27 of the NPRM, SBC questions the need for a requirement to report compromises of confidentiality and of illegal wiretapping. Given the historic emphasis placed by SBC companies on protecting the privacy of customers' communications, and on

maintaining the confidentiality of their cooperation with law enforcement, such incidents have been, and are likely in the future to be, extremely rare.

Under existing procedures, both the security of information regarding the placement of surveillance and the public interest in preventing unlawful surveillance are well protected. For example, when the Southwestern Bell Security or Pacific Bell Investigative Services organizations receive a lawfully authorized surveillance order, knowledge thereof is restricted on a "need to know" basis, to only those employees who must be aware of the surveillance in order for it to be effectuated. All such employees are instructed in each case that no disclosure of the matter is to occur except to the Security or Investigative Services personnel involved. Moreover, technicians are trained to recognize non-standard devices that may be attached to SBC facilities in central offices or in the field, and are under standing instructions to report such devices immediately to the appropriate Security or Investigative Services group. These groups, in turn, verify whether the device has been placed pursuant to a proper court order or other lawful authorization, and if not, the existence and location of the unlawful surveillance device are reported immediately to local law enforcement authorities. In the extremely rare event that one or more employees of SBC companies are found to have been involved in the placement, use or maintenance of an illegal surveillance device, or are found to have improperly disclosed the existence of properly authorized surveillance, such employees are subject to immediate disciplinary action, which normally means termination of employment. SBC companies have extensive and strictly

enforced compliance programs and codes of business conduct which supplement and support these procedures.

SBC sees no logical grounds for any contention that compliance with an FCC reporting requirement could or should serve to modify or mitigate a carrier's liability under 18 U.S.C. §2511 and/or §2520. Whatever value such a reporting requirement might have, SBC believes that an FCC rule establishing such a requirement cannot, without express direction from Congress, operate to alter or modify civil and criminal liabilities that might arise under these pre-existing statutes. No such direction is to be found anywhere in CALEA.

If reporting rules nevertheless are imposed, SBC believes that the FCC should not require carriers to report illegal wiretapping and compromises of confidentiality of interception to the FCC in any case, as there is no apparent need for such a requirement. As a matter of course, any court order or other legal authority for a wiretap, pen register or trap and trace device ordinarily contains an admonition against disclosure of the existence and/or contents of the interception, and the enabling statutes (*e.g.*, 18 U.S.C. §2520) provide both civil and criminal penalties for such disclosure. Thus, the only reporting procedure needed to effectuate the purposes of these statutory restrictions would provide for reporting breaches to the court that issued the underlying order, and/or to the affected law enforcement agency or agencies. As noted previously, SBC companies already have established practices that require such reporting to LEAs. Further, any such reporting requirement should, in the interests of fairness, be limited to those breaches reasonably within the carrier's

ability to detect. For example, there is no technology in place today that would enable carriers automatically to detect an unauthorized wiretap such as a handset attached to a terminal box or distribution frame. In any event, if reports to the FCC nonetheless are required, they should be required only on a strictly confidential basis.

D. Prohibiting Carrier Assistance To LEAs Prior To Actual Receipt Of A Court Order Could Unnecessarily Delay Implementation Of Lawful Surveillance.

SBC agrees, except as noted immediately below, with the FCC's tentative conclusion, in Paragraph 29 of the NPRM, that "appropriate legal authorization for purposes of CALEA encompasses what is required by §2518 of Title 18 of the United States Code." SBC also agrees that existing law adequately protects citizens' privacy and security rights against improper surveillance. It therefore would be superfluous for the FCC to impose a rule requiring carriers to state in their internal policies and procedures that a court order or other certification must be received before the carrier's employees may render any assistance to law enforcement officials in implementing electronic surveillance.

The FCC should note, however, that the proposal in Paragraph 29 apparently fails to recognize the distinction between interceptions of wire and oral communications under 18 U.S.C. §2518 (generally referred to as "Title III orders") and the use of pen register or trap and trace devices pursuant to 18 U.S.C. §3121 *et seq.* Only the former are subject to the detailed requirements referred to in Paragraph 29, and these "Title III" orders represent less than ten percent of the thousands of surveillance orders processed annually by SBC

companies.[7] All other surveillance orders are for pen register or trap and trace devices, which do not intercept the content of communications, and as to which the requirements for obtaining a court order are far less extensive.[8] The FCC would cause a severe and unwarranted burden on LEAs, as well as on carriers, by imposing all of the requirements of a "Title III" order on each and every instance of electronic surveillance. Not incidentally, such a rule also would likely be unenforceable, as it would have the effect of amending the clear language of the cited statutes, something the FCC is entirely without authority to do.

Even if properly limited to "Title III" orders, the proposed rule prohibiting any carrier assistance to LEAs prior to actual receipt of a court order could cause unnecessary delays in implementing lawful surveillance, to the detriment of law enforcement investigations. Due to the high level of trust and credibility that has been established over the years between SBC and the LEAs with which SBC companies cooperate, much of the technical work needed to establish lawful surveillance is routinely performed based on written requests received prior to actual receipt of the court order, which requests include the agencies' assurance that a proper court order is being sought. Of course, no surveillance information is actually made available to law enforcement officials until the appropriate court order or other statutory authorization has been received, but in

---

[7] Thus far in 1997, for example, Southwestern Bell Telephone Company's Security organization has processed over 1,400 court-ordered surveillance requests for LEAs, of which only 101 were Title III interception orders. Similarly, through October, 1997, Pacific Bell Investigative Services has processed approximately 2,500 court-ordered surveillance requests, of which fewer than five percent involved Title III voice interception.

[8] 18 U.S.C. §2511(2)(h) exempts properly authorized pen register/trap and trace device usage from the requirements applied to Title III orders. 18 U.S.C. §3122(b) sets forth the requirements for issuance of a court order authorizing installation and use of pen registers and trap and trace devices.

most cases (excepting "trap and trace" situations, which require no special preparation), it takes at least a day or two, and sometimes as much as seven to ten working days, for all the necessary connections and facility assignments to be put in place to enable the surveillance. If such preparatory work is deemed to constitute "assistance" under CALEA and related laws, a proposition with which SBC does not agree, then in cases not involving emergency circumstances, the proposed rule could postpone the implementation of the surveillance for so long as it takes to make the necessary technical preparations, quite possibly resulting in the loss of critical evidence for the Government. This would be a lesser level of cooperation with LEAs than carriers ordinarily provide today, a result SBC does not believe Congress intended.

IV. The SBC Companies' Current Security And Record-Keeping Policies Adequately Provide For Security, Confidentiality And Accurate Documentation Of Electronic Surveillance Activity.

A. Specific Rules Governing Employee Conduct Are Unnecessary.

Section 229 of the Communications Act requires the FCC to establish only such rules as are necessary in order to implement the requirements of CALEA. The FCC correctly acknowledges that carriers who historically have been providing assistance to LEAs already have in place practices for proper employee conduct and record keeping. (NPRM, Paragraph 74.) SBC companies have well-established policies in this regard. Thus, rather than adopting the proposed rules to govern employee conduct, (NPRM, Paragraph 29), the FCC should implement its stated position and provide "general guidance

regarding the conduct of carrier personnel and the content of records in this NPRM." (NPRM, Paragraph 74.)

As described in Section III, above, SBC's current internal policies and procedures governing employee conduct satisfy the need for security and confidentiality. SBC has dedicated organizations in its companies which are responsible for ensuring that its assistance in electronic surveillance activity is well managed and protects the privacy and confidentiality of both the communications intercepted and the interception activity itself. These organizations also are responsible for ensuring that any surveillance devices placed in SBC facilities are lawfully authorized, and that when detected, unlawful devices are immediately removed and reported to the appropriate LEA. SBC companies require LEAs to present a court order or other lawful authorization before SBC companies will provide LEAs with the means to obtain information gathered via electronic surveillance activity. (NPRM, Paragraph 29.) These long-established procedures have been proven successful in providing assistance to LEAs over many years, and SBC is unaware of any recent or pending complaints by any LEA concerning such procedures or breaches of their confidentiality. The FCC should accept the time proven policies and procedures carriers have established, and should impose additional rules only if and when a carrier is found to have been repeatedly unable or unwilling properly to preserve the goals of CALEA and the related electronic surveillance provisions of Title 18, United States Code. (NPRM, Paragraph 30.)

B. The Proposed Rules Requiring Designation And Listing Of Employees Permitted To Participate In Enabling LEA Surveillance Activities Are Unnecessary And Overly Burdensome.

The FCC's proposed rule limiting participation in lawful surveillance activities to a few designated employees should not be adopted. Such a rule would be cumbersome and impractical, at best, given the operational structure of SBC and other carriers, and the unpredictable nature of the incidence of lawful surveillance activities. Because there currently is no technologically feasible way to centralize the "hardware" components of surveillance activities, the actual placement of facilities that enable LEAs to activate interceptions, pen registers and trap and trace devices can occur virtually anywhere in the network, depending upon the location of the existing facilities that serve the target party.[9] Thus, nearly every employee in a carrier's customer service, network engineering and network craft organizations might at some point need to be involved in one of the many technical steps required to effect lawful surveillance activities.[10] To attempt to limit such activities to a few designated employees

[9] In approximately half of all cases, the actual placement of interception devices is done by LEA personnel in the field, who attach hardware to the network at a location proximate to the physical location of the target communication service. In these instances, the role of the carrier is to set up the necessary circuits to enable this procedure, and to inform the LEA personnel of the appropriate location for their device. In other cases, the surveillance device actually is placed in a carrier's switching office by carrier personnel, who also set up the circuits which permit LEA personnel to "dial up" the surveillance device from their own chosen locations. In still other cases, primarily involving "trap and trace" orders, carrier personnel simply gather data routinely generated by the switching system for any call and forward that data to LEA personnel.

[10] In many instances, the employee performing this work has no way of knowing that he or she is helping to implement a court-ordered interception. In many other cases, however, just the opposite is true. Existing procedures in SBC companies, for example, require that the Security or Investigative Services organization be listed as the contact for matters involving the implementation of court-ordered surveillance. Most employees are astute enough to infer from this fact that such a work order involves surveillance activity. In other instances, such as where a pen register or voice intercept is activated, the procedure often involves placement of a small hardware device on the distribution frame in the central

would cause undue delays in the effectuation of the surveillance, since it no longer would be possible to assign various steps of the process to the most readily available employees. Restricting the number of employees who could be assigned these tasks also would increase the likelihood that delays would be caused by employee turnover, absences due to vacations and illness, and the like. Further, the fewer persons designated, the more difficult it would be for law enforcement to receive twenty-four hour, seven-day access to carrier assistance and information, especially in emergency situations.

Finally, the Commission should not require lists to be made and kept of all employees involved in all of the several thousand surveillance orders handled each year. As noted above, such a requirement is unrealistic because of the sheer number of employees who might be involved. In addition, compiling lists of such employees would call attention to the purpose of the work being done by those employees who otherwise might be unaware that the purpose of their work is related to assisting LEA surveillance.

C. Requiring Individual Affidavits For Every Surveillance Event Is Overly Burdensome And Unnecessary. Existing Record Keeping Procedures Are Sufficient To Meet Any Reasonable Documentation Requirement.

SBC strongly urges the FCC to refrain from imposing a rule that requires the execution of a separate affidavit by every employee who knowingly participates in the implementation of lawfully authorized surveillance. As noted repeatedly herein, there are several thousand surveillance orders handled

---

office. (See Note 7, supra.). Any carrier employee in the immediate vicinity of the frame who has technical expertise and sees such a device would immediately know its purpose.

annually by SBC companies. Requiring the proposed affidavit procedure would thus generate many thousands of pages of documentation per year, requiring countless hours of labor and causing carriers to incur significant costs for preparation and storage thereof. Such a requirement is especially uncalled for given the fact that no serious difficulties have been noted in the industry's ability to maintain the appropriate level of internal control and confidentiality regarding carriers' assistance to LEAs. At the very least, before imposing such onerous administrative burdens on the industry, the FCC should cite persuasive examples of problems that demonstrate a clear need for this proposal. If active affirmation of confidentiality by employees involved in surveillance nevertheless is deemed necessary, designated employees should only be required to sign a nondisclosure statement once, when they begin their functions in the designated organization.

Similarly, the proposed requirement for a second set of records to be generated contemporaneously with, or within 48 hours after, the initiation of surveillance is extreme and unnecessary. Except for the identification of all employees who are involved in the process of facilitating a surveillance, SBC's existing records (including the court order or other legal authorization and one or two routine work order documents) already contain all of the information spelled out in Paragraph 32 of the NPRM (subject to the qualifications noted immediately below, with respect to "start date and time" and "stop date and time"

of surveillance.) SBC submits that its existing records[11] should be deemed sufficient to meet any FCC requirements in this area, perhaps supplemented by an identification of the manager primarily responsible for initiating the process of enabling surveillance. In SBC's case, this would be an employee in the centralized Court Order Bureau, which handles all LEA surveillance requests in the first instance, and issues appropriate directives to field personnel in accordance with each court order or other lawful authorization received from an LEA. Again, SBC reiterates that there have been no problems experienced in the past which would justify the huge increase in record keeping labor and costs that would be generated by the FCC's proposed rule.

In any event, the FCC should note that it is impossible for carriers even to know, much less keep separate records of, the "start date and time" and "stop date and time" of an interception, if by these terms the FCC means the actual time when dialed digits or voice transmissions are being monitored or recorded pursuant to a court order. (NPRM, Paragraph 32.) In most cases, SBC companies merely open a circuit for law enforcement, and no SBC employee has any way to know precisely when the law enforcement agency begins or ends the actual interception.[12] In these instances, SBC is able to maintain records relating only to the date and time that each such circuit is made available, and the date and time when circuit is "taken down", which will reflect the effective

[11] SBC agrees that the term for retaining records of electronic surveillance activity should be same as the term required to retain the intercepted communication-ten years, pursuant to 18 U.S.C. §2518(8)(a).
[12] With respect to "trap and trace" orders, since all of the information flow is controlled by carrier personnel, it is possible for a carrier to note and document the first and last transmissions of data to law enforcement. Existing records are already sufficient for this purpose, however.